LIST OF CLAIMS / AMENDMENTS

In the Claims

Claims 8-9, 33-36, and 71-75 were previously canceled.

Please cancel claims 30-31, 42-43, and 66-67 without prejudice.

Please amend claims 1, 15, 20, 25, 32, 37, 44, 61, and 68 as shown herein.

Claims 1-7, 10-29, 32, 37-41, 44-65, and 68-70 are pending and are listed following:

1. (currently amended) A network system, comprising:

a first device to maintain an original resource;

a second device to maintain a replica resource remotely from the first device, the replica resource being replicated from the original resource;

memory to store a cached descriptor corresponding to the original resource;

a security component to determine whether a request for the replica resource will pose a security risk to the second device where the request designates a resource locator, the security component further configured to determine whether the replica resource will pose a security risk to the second device upon receipt of a request for the replica resource, ~~wherein the request designates a resource locator,~~ the security component configured to:

~~being configured to determine whether the request will pose a security risk to the second device;~~

~~formulating~~ formulate a descriptor corresponding to the replica resource and ~~comparing~~ compare the formulated descriptor with the cached descriptor; and if the formulated descriptor and the cached descriptor are not equivalent, ~~formulating~~ formulate a second descriptor corresponding to the original resource and ~~comparing~~ compare the formulated descriptor with the second descriptor.

2. **(original)** A network system as recited in claim 1, wherein the security component determines that the replica resource is not a security risk if the formulated descriptor and the cached descriptor are equivalent.

3. **(original)** A network system as recited in claim 1, wherein, if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are equivalent, the security component determines that the replica resource is not a security risk.

4. **(original)** A network system as recited in claim 1, wherein, if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are equivalent, the security component determines that the replica resource is not a security risk, and the cached descriptor is replaced with the second descriptor.

5. (original) A network system as recited in claim 1, wherein, if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are not equivalent, the security component determines that the replica resource is a security risk, and the replica resource is replaced with a copy of the original resource.

6. (original) A network system as recited in claim 1, wherein, if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are not equivalent, the security component determines that the replica resource is a security risk, the replica resource is replaced with a copy of the original resource, and the cached descriptor is replaced with the second descriptor.

7. (original) A network system as recited in claim 1, wherein the security component formulates the cached descriptor when the original resource is replicated to create the replica resource.

8-9. (canceled)

10. (previously presented) A network system as recited in claim 1, wherein the request further designates the resource locator having a resource path, the resource path identifying a location of the replica resource, and wherein the security component determines that the request is not a security risk if the resource path does not exceed a maximum number of characters.

11. (previously presented) A network system as recited in claim 1, wherein the request further designates the resource locator having a plurality of arguments, and wherein the security component determines that the request is not a security risk if individual arguments do not exceed a maximum number of characters, and if a total number of characters defining all of the arguments do not exceed a maximum number of characters.

12. (previously presented) A network system as recited in claim 1, wherein the request further designates the resource locator having a resource identifier, and wherein the security component determines that the request is not a security risk if the resource identifier has a valid file extension.

13. (previously presented) A network system as recited in claim 1, wherein:

the request further designates the resource locator having a resource path and one or more arguments, the resource path identifying a location of the replica resource and the resource path having a resource identifier;

the security component determines that the request is not a security risk if:

the resource path does not exceed a maximum number of characters;

individual arguments do not exceed a maximum number of characters;

a total number of characters defining all of the arguments do not exceed a maximum number of characters; and

the resource identifier has a valid file extension.

14. (previously presented) A network server, comprising:

a server component to receive a request for a resource maintained on the network server and, in response to the request, implement security policies to prevent unauthorized access to the resource;

a memory to store a cached descriptor corresponding to the resource; and

a security component that is registerable with the server component during run-time to determine whether the request will pose a security risk to the network server, the request posing the security risk if the resource has been corrupted and if execution of the resource will compromise the network server, the security component being configured to:

formulate a replica descriptor corresponding to a replica of the resource and compare the replica descriptor with the cached descriptor; and

if the replica descriptor and the cached descriptor are not equivalent, formulate a second descriptor corresponding to the resource and compare the replica descriptor with the second descriptor.

15. (currently amended) A network server as recited in claim 14, wherein, if the security component determines that the request will pose a security risk <u>to the network server</u>, the security component redirects the request to indicate that the resource is not available.

16. (original) A network server as recited in claim 14, wherein the request designates a resource locator having a resource path, the resource path identifying a location of the resource, and wherein the security component determines that the request is not a security risk if the resource path does not exceed a maximum number of characters.

17. (original) A network server as recited in claim 14, wherein the request designates a resource locator having a plurality of arguments, and wherein the security component determines that the request is not a security risk if individual arguments do not exceed a maximum number of characters, and if a total number of characters defining all of the arguments do not exceed a maximum number of characters.

18. (original) A network server as recited in claim 14, wherein the request designates a resource locator having a resource identifier, and wherein the security component determines that the request is not a security risk if the resource identifier has a valid file extension.

19. (original) A network server as recited in claim 14, wherein:

the request designates a resource locator having a resource path and one or more arguments, the resource path identifying a location of the resource and the resource path having a resource identifier;

the security component determines that the request is not a security risk if:

the resource path does not exceed a maximum number of characters;

individual arguments do not exceed a maximum number of characters;

a total number of characters defining all of the arguments do not exceed a maximum number of characters; and

the resource identifier has a valid file extension.

20. (currently amended) A network server system, comprising:

a server component in a network server to receive a request for a resource maintained on the network server, the request designating a resource locator having a resource path that identifies a location of the resource, and, in response to the request, implement security policies to prevent unauthorized access to the resource;

a memory to store a cached descriptor corresponding to the resource; and

a security component in a computing device remote to the network server and registerable with the server component during run-time to determine whether the resource will pose a security risk to the network server upon receipt of the request, the security component being configured to:

formulate a replica descriptor corresponding to a replica of the resource and compare the replica descriptor with the cached descriptor; and

if the replica descriptor and the cached descriptor are not equivalent, formulate a second descriptor corresponding to the ~~original~~ resource and compare the replica descriptor with the second descriptor.

21. (previously presented) A network server system as recited in claim 20, wherein, if the security component determines that the resource will pose a security risk, the security component redirects the request to indicate that the resource is not available.

22. (previously presented) A network server system as recited in claim 20, wherein the security component:

formulates a descriptor corresponding to the resource;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested; and

determines that the resource is not a security risk if the formulated descriptor and the cached descriptor are equivalent.

23. (previously presented) A network server system as recited in claim 20, wherein the security component:

formulates a descriptor corresponding to the resource;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;

if the formulated descriptor and the cached descriptor are not equivalent, formulates a second descriptor corresponding to an original resource maintained on a file server remotely located from the network server, the resource being replicated from the original resource;

compares the formulated descriptor with the second descriptor; and

determines that the resource is not a security risk if the formulated descriptor and the second descriptor are equivalent.

24. (previously presented) A network server system as recited in claim 20, wherein the security component:

formulates a descriptor corresponding to the resource;

compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;

if the formulated descriptor and the cached descriptor are not equivalent, formulates a second descriptor corresponding to an original resource maintained on a file server remotely located from the network server, the resource being replicated from the original resource;

compares the formulated descriptor with the second descriptor;

if the formulated descriptor and the second descriptor are not equivalent, initiates that the resource stored on the network server be replaced with a copy of the original resource maintained on the file server; and

initiates that the cached descriptor be replaced with the second descriptor.

25. (currently amended) A network server, comprising:

an Internet server to receive a request for a resource maintained on the network server and, in response to the request, implement security policies to prevent unauthorized access to the resource;

a security component that is registerable with the Internet server during run-time, the security component having:

a validation component to determine whether the request will pose a security risk to the network server by determining if a total number of characters defining all of the arguments of the request exceeds a maximum number of characters; and

an integrity verification component to:

determine whether the resource will pose a security risk to the network server upon receipt of the request;

formulate a descriptor corresponding to the resource;

compare the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;

determine that the resource is not a security risk if the formulated descriptor and the cached descriptor are equivalent;

if the formulated descriptor and the cached descriptor are not equivalent, formulate a second descriptor corresponding to an original resource maintained on a file server remotely located from the network server, the resource being replicated from the original resource;

compare the formulated descriptor with the second descriptor; and

determine that the resource is not a security risk if the formulated descriptor and the second descriptor are equivalent.

26. **(original)** A network server as recited in claim 25, wherein the request designates a resource locator having a resource path, the resource path identifying a location of the resource, and wherein the validation component determines that the request is not a security risk if the resource path does not exceed a maximum number of characters.

27. **(previously presented)** A network server as recited in claim 25, wherein the request designates a resource locator having a plurality of arguments, and wherein the validation component determines that the request is not a security risk if individual arguments do not exceed a maximum number of characters.

28. **(original)** A network server as recited in claim 25, wherein the request designates a resource locator having a resource identifier, and wherein the validation component determines that the request is not a security risk if the resource identifier has a valid file extension.

29. (previously presented) A network server as recited in claim 25, wherein:

the request designates a resource locator having a resource path and one or more arguments, the resource path identifying a location of the resource and the resource path having a resource identifier;

the validation component determines that the request is not a security risk if:

the resource path does not exceed a maximum number of characters;

individual arguments do not exceed a maximum number of characters; and

the resource identifier has a valid file extension.

30-31. (canceled)

32. (currently amended) A network server as recited in claim 25, wherein if the formulated descriptor and the second descriptor are not equivalent, the integrity verification component:

~~formulates a descriptor corresponding to the resource;~~

~~compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;~~

~~if the formulated descriptor and the cached descriptor are not equivalent,~~

~~formulates a second descriptor corresponding to an original resource maintained on a file server remotely located from the network server, the resource being replicated from the original resource;~~

~~compares the formulated descriptor with the second descriptor;~~

~~if the formulated descriptor and the second descriptor are not equivalent,~~

initiates that the resource stored on the network server be replaced with a copy of the original resource maintained on the file server; and

initiates that the cached descriptor be replaced with the second descriptor.

33-36. (canceled)

37. (currently amended) One or more computer readable media containing a security application, comprising:

a validation component to determine whether a request for a resource poses a security risk by determining if a total number of characters defining all of the arguments of the request exceeds a maximum number of characters; and

an integrity verification component to determine whether the resource poses a security risk, the integrity verification component further configured to:

formulate a descriptor corresponding to the resource when the security application receives the request;

compare the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;

if the formulated descriptor and the cached descriptor are not equivalent, formulate a second descriptor corresponding to an original resource remotely located, the resource being replicated from the original resource;

compare the formulated descriptor with the second descriptor; and

determine that the resource is not a security risk if the formulated descriptor and the second descriptor are equivalent.

38. (original) Computer readable media as recited in claim 37, wherein the request designates a resource locator having a resource path, the resource path identifying a location of the resource, and wherein the validation component determines that the request is not a security risk if the resource path does not exceed a maximum number of characters.

39. (previously presented) Computer readable media as recited in claim 37, wherein the request designates a resource locator having a plurality of arguments, and wherein the validation component determines that the request is not a security risk if individual arguments do not exceed a maximum number of characters.

40. (original) Computer readable media as recited in claim 37, wherein the request designates a resource locator having a resource identifier, and wherein the validation component determines that the request is not a security risk if the resource identifier has a valid file extension.

41. (previously presented) Computer readable media as recited in claim 37, wherein:

the request designates a resource locator having a resource path and one or more arguments, the resource path identifying a location of the resource and the resource path having a resource identifier;

the validation component determines that the request is not a security risk if:

the resource path does not exceed a maximum number of characters;

individual arguments do not exceed a maximum number of characters; and

the resource identifier has a valid file extension.

42-43. (canceled)

44. (currently amended) Computer readable media as recited in claim 37, wherein if the formulated descriptor and the second descriptor are not equivalent, the integrity verification component:

~~formulates a descriptor corresponding to the resource when the security application receives the request;~~

~~compares the formulated descriptor with a cached descriptor, the cached descriptor corresponding to the resource and formulated when the resource is initially requested;~~

~~if the formulated descriptor and the cached descriptor are not equivalent, formulates a second descriptor corresponding to an original resource remotely located, the resource being replicated from the original resource;~~

~~compares the formulated descriptor with the second descriptor;~~

~~if the formulated descriptor and the second descriptor are not equivalent,~~

initiates that the resource be replaced with a copy of the original resource; and

initiates that the cached descriptor be replaced with the second descriptor.

45. (previously presented) A method, comprising:

receiving a request for a replica resource stored on a computing device, the request designating a resource locator having a resource path identifying a location of the replica resource;

formulating a descriptor corresponding to the replica resource;

comparing the formulated descriptor with a cached descriptor corresponding to an original resource stored on a second computing device remotely located from the computing device, the replica resource being replicated from the original resource;

determining that the replica resource does not pose a security risk if the formulated descriptor and the cached descriptor are equivalent;

if the formulated descriptor and the cached descriptor are not equivalent, formulating a second descriptor corresponding to the original resource;

comparing the formulated descriptor with the second descriptor; and

determining that the replica resource does not pose a security risk if the formulated descriptor and the second descriptor are equivalent.

46. (original) A method as recited in claim 45, further comprising allowing the request if said determining that the replica resource does not pose a security risk to the computing device.

47. (original) A method as recited in claim 45, further comprising redirecting the request to indicate that the replica resource is not available if determining that the replica resource poses a security risk to the computing device.

48. (original) A method as recited in claim 45, further comprising replacing the cached descriptor with the second descriptor if the formulated descriptor and the second descriptor are equivalent.

49. (original) A method as recited in claim 45, further comprising replacing the replica resource with a copy of the original resource if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are not equivalent.

50. (original) A method as recited in claim 45, further comprising replacing the cached descriptor with the second descriptor if the formulated descriptor and the cached descriptor are not equivalent, and if the formulated descriptor and the second descriptor are not equivalent.

51. (original) A method as recited in claim 45, further comprising formulating the cached descriptor when the original resource is replicated to create the replica resource.

52. (original) A method as recited in claim 45, further comprising formulating the cached descriptor when the replica resource is initially requested.

53. (original) A method as recited in claim 45, further comprising determining whether the request will pose a security risk.

54. (original) A method as recited in claim 45, further comprising:

determining whether the request will pose a security risk; and

redirecting the request to indicate that the replica resource is not available if determining that the request poses a security risk to the computing device.

55. (previously presented) A method as recited in claim 45, further comprising determining that the request does not pose a security risk if the resource path does not exceed a maximum number of characters.

56. (previously presented) A method as recited in claim 45, wherein the request further designates the resource locator having a plurality of arguments, and the method further comprising determining that the request does not pose a security risk if individual arguments do not exceed a maximum number of characters, and if a total number of characters defining all of the arguments do not exceed a maximum number of characters.

57. (previously presented) A method as recited in claim 45, wherein the request further designates the resource locator having a resource identifier, and the method further comprising determining that the request does not pose a security risk if the resource identifier has a valid file extension.

58. (previously presented) A method as recited in claim 45, wherein:

the request further designates the resource locator having a resource path and one or more arguments, the resource path identifying a location of the replica resource and the resource path having a resource identifier;

the method further comprising determining that the request does not pose a security risk if:

the resource path does not exceed a maximum number of characters;

individual arguments do not exceed a maximum number of characters;

a total number of characters defining all of the arguments do not exceed a maximum number of characters; and

the resource identifier has a valid file extension.

59. (original) A computer-readable medium comprising computer executable instructions that, when executed, direct a computing system to perform the method of claim 45.

60. (original) A computer-readable medium comprising computer executable instructions that, when executed, direct a computing system to perform the method of claim 58.

61. (currently amended) A method, comprising:

receiving a request for a resource;

implementing security policies to prevent unauthorized access to the resource;

determining whether the request will pose a security risk by determining if a total number of characters defining all of the arguments of the request exceeds a maximum number of characters; and

determining whether the resource will pose a security risk if allowing the request;

formulating a descriptor corresponding to the resource;

comparing the formulated descriptor with a cached descriptor corresponding to the resource and formulated when the resource is initially requested;

determining that the resource does not pose a security risk if the formulated descriptor and the cached descriptor are equivalent;

if the formulated descriptor and the cached descriptor are not equivalent, formulating a second descriptor corresponding to an original resource remotely located, the resource replicated from the original source;

comparing the formulated descriptor with the second descriptor; and

determining that the resource does not pose a security risk if the formulated descriptor and the second descriptor are equivalent.

62. (original) A method as recited in claim 61, further comprising allowing the request for the resource if determining that the request does not pose a security risk and if determining that the resource does not pose a security risk.

63. (original) A method as recited in claim 61, wherein the request designates a resource locator having a resource path, the resource path identifying a location of the resource, and the method further comprising determining that the request does not pose a security risk if the resource path does not exceed a maximum number of characters.

64. (previously presented) A method as recited in claim 61, wherein the request designates a resource locator having a plurality of arguments, and the method further comprising determining that the request does not pose a security risk if individual arguments do not exceed a maximum number of characters.

65. (original) A method as recited in claim 61, wherein the request designates a resource locator having a resource identifier, and the method further comprising determining that the request does not pose a security risk if the resource identifier has a valid file extension.

66-67. (canceled)

68. (currently amended) A method as recited in claim 61, further comprising:

~~formulating a descriptor corresponding to the resource;~~

~~comparing the formulated descriptor with a cached descriptor corresponding to the resource and formulated when the resource is initially requested;~~

~~determining that the resource does not pose a security risk if the formulated descriptor and the cached descriptor are equivalent;~~

~~if the formulated descriptor and the cached descriptor are not equivalent, formulating a second descriptor corresponding to an original resource remotely located, the resource replicated from the original resource;~~

~~comparing the formulated descriptor with the second descriptor; and~~

~~determining that the resource does not pose a security risk if the formulated descriptor and the second descriptor are equivalent;~~

if the formulated descriptor and the second descriptor are not equivalent, replacing the resource with a copy of the original resource and replacing the cached descriptor with the second descriptor.

69. (original) A computer-readable medium comprising computer executable instructions that, when executed, direct a computing system to perform the method of claim 61.

70. (original) A computer-readable medium comprising computer executable instructions that, when executed, direct a computing system to perform the method of claim 68.

71-75. (canceled)